



3.

Auflage

Christian Johner · Matthias Hölzer-Klüpfel · Sven Wittorf

Basiswissen Medizinische Software

Aus- und Weiterbildung
zum Certified Professional
for Medical Software



dpunkt.verlag



Professor **Christian Johner** unterrichtete an mehreren Hochschulen u.a. in Konstanz, Würzburg, Krems, St. Gallen und Stanford Software Engineering, Softwarearchitektur, Softwarequalitätssicherung und Medizinische Informatik. Am Johner Institut bildet er promovierte Physiker im Rahmen von berufsbegleitenden Masterstudiengängen und Seminaren Personen aus, die IT-Lösungen für das Gesundheitswesen entwickeln, prüfen, anwenden und betreiben. Mit seiner Firma berät er Medizinproduktehersteller bei der Entwicklung, Qualitätssicherung und Zulassung von medizinischer Software.



Matthias Hölzer-Klüpfel studierte Physik an der Universität Würzburg. Seit 2002 ist er als Entwickler, Berater und Projektleiter tätig. Er führte zahlreiche Projekte im Bereich Medizintechnik durch und war dabei sowohl bei KMU-Firmen als auch in Großunternehmen im Einsatz. Heute ist er freiberuflicher Berater und unterstützt seine Kunden bei Fragen rund um die Software- und Systementwicklung in der Medizintechnik. Neben seinen beruflichen Tätigkeiten schloss er im Juli 2009 den Masterstudiengang »IT im Gesundheitswesen« ab. Matthias Hölzer-Klüpfel ist Mitbegründer des Vereins »ICPMSB e.V.«, der die Grundlagen für die Zertifizierungen zum »Certified Professional for Medical Software« erarbeitet, und Vorsitzender des Fachausschusses »Software in der Medizintechnik« im Verein Deutscher Ingenieure (VDI).



Sven Wittorf hat Elektro- und Informationstechnik an der TU Darmstadt studiert und einen Abschluss als Master of Science im Bereich IT im Gesundheitswesen. Seit 2012 ist er geschäftsführender Gesellschafter der Medsoto GmbH, die Softwarewerkzeuge zur Unterstützung des normenkonformen Arbeitens in der Medizintechnik erstellt. Er ist Gründungsmitglied des ICPMSB e.V. und Mitglied im nationalen Normungsgremium der IEC 62304 sowie im VDI-Fachausschuss »Qualitätssicherung für Software in der Medizintechnik«. Für das Johner Institut arbeitet er als Trainer für das CPMS-Programm.

Christian Johner · Matthias Hölzer-Klüpfel · Sven Wittorf

Basiswissen Medizinische Software

**Aus- und Weiterbildung zum
Certified Professional for Medical Software**

Unter Mitarbeit von
Thomas Geis, Dr. Christof Gessner und Markus Manleitner

3., überarbeitete und aktualisierte Auflage



dpunkt.verlag

Christian Johner
christian.johner@johner-institut.de

Matthias Hölzer-Klüpfel
matthias@hoelzer-kluepfel.de

Sven Wittorf
sven.wittorf@medsoto.de

Lektorat: Christa Preisendanz
Copy-Editing: Ursula Zimpfer, Herrenberg
Satz: Birgit Bäuerlein
Herstellung: Stefanie Weidner
Umschlaggestaltung: Helmut Kraus, *www.exclam.de*
Druck und Bindung: mediaprint solutions GmbH, 33100 Paderborn

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie;
detaillierte bibliografische Daten sind im Internet über *http://dnb.d-nb.de* abrufbar.

ISBN:
Print 978-3-86490-743-2
PDF 978-3-96910-057-8
ePub 978-3-96910-058-5
mobi 978-3-96910-059-2

3., überarbeitete und aktualisierte Auflage 2021
Copyright © 2021 dpunkt.verlag GmbH
Wieblinger Weg 17
69123 Heidelberg

Hinweis:

Dieses Buch wurde auf PEFC-zertifiziertem Papier aus nachhaltiger Waldwirtschaft gedruckt. Der Umwelt zuliebe verzichten wir zusätzlich auf die Einschweißfolie.



Schreiben Sie uns:

Falls Sie Anregungen, Wünsche und Kommentare haben, lassen Sie es uns wissen: *hallo@dpunkt.de*.

Die vorliegende Publikation ist urheberrechtlich geschützt. Alle Rechte vorbehalten. Die Verwendung der Texte und Abbildungen, auch auszugsweise, ist ohne die schriftliche Zustimmung des Verlags urheberrechtswidrig und daher strafbar. Dies gilt insbesondere für die Vervielfältigung, Übersetzung oder die Verwendung in elektronischen Systemen.

Es wird darauf hingewiesen, dass die im Buch verwendeten Soft- und Hardware-Bezeichnungen sowie Markennamen und Produktbezeichnungen der jeweiligen Firmen im Allgemeinen warenzeichen-, marken- oder patentrechtlichem Schutz unterliegen.

Alle Angaben und Programme in diesem Buch wurden mit größter Sorgfalt kontrolliert. Weder Autor noch Verlag können jedoch für Schäden haftbar gemacht werden, die in Zusammenhang mit der Verwendung dieses Buches stehen.

5 4 3 2 1 0

Vorwort zur 3. Auflage

Die Welt des Medizinprodukterechts dreht sich weiterhin schnell: Die EU-Medizinprodukteverordnungen (MDR und IVDR) haben die EU-Richtlinien weitestgehend abgelöst. Für die Hersteller bedeutet(e) dieser Umstieg eine hohe Belastung, zumal sich die Anzahl der benannten Stellen mehr als halbiert und damit die Verfügbarkeit benannter Stellen stark beeinträchtigt hat.

Für die Firmen und deren Mitarbeitende bleibt es herausfordernd, mit den Interpretationen der neuen Verordnungen, mit den Updates der Normen (z.B. zu den Software-Lebenszyklus-Prozessen und zur Gebrauchstauglichkeit), mit den neuen EU-Leitlinien sowie den Common Specifications Schritt zu halten.

Gleichzeitig nimmt der internationale Wettbewerb zu, neue Themen wie die künstliche Intelligenz und das Internet of Things wollen verstanden und beherrscht sein, und die Entwicklungszyklen werden immer kürzer.

Daher ist es wichtig, dass die Entwicklung medizinischer Software nicht durch unnötige QM-Bürokratie und missverstandene Regularien behindert wird.

Die dritte Auflage dieses Buches soll einen Beitrag dazu leisten, dass Firmen Medizinprodukte, die Software enthalten oder selbst Software sind, schnell, sicher und gesetzeskonform entwickeln können und damit im Markt erfolgreich und den Patienten dienlich sind.

Das Buch wurde um die Veränderungen und Neuerungen seit der letzten Auflage erweitert sowie an den aktualisierten Lehrplan des CPMS-Programms angepasst. Dadurch ist ein weiteres Kapitel zum Thema IT-Sicherheit hinzugekommen. Die bewährte Struktur des Kapitels zu den rechtlichen Grundlagen wurde beibehalten, alle Informationen wurden aber um die Inhalte der neuen Medizinprodukteverordnung ergänzt. Wir haben uns bewusst dazu entschieden, die Anforderungen der drei Richtlinien für Medizinprodukte noch nicht komplett aus dem Inhalt zu entfernen, da diese durch Übergangsfristen und möglicherweise weitere Verschiebungen noch mehrere Jahre relevant sein könnten.

Christian Johner, Matthias Hölzer-Klüpfel, Sven Wittorf
Konstanz, Würzburg, Seeheim-Jugenheim, im August 2020

Vorwort zur 2. Auflage

Viel hat sich ereignet seit der ersten Auflage dieses Buches:

Skandale, wie der Einsatz gesundheitsgefährdender Brustimplantate, haben die Medizinproduktwelt aufgerüttelt, mit Folgen, deren Tragweite noch immer nicht ganz abschätzbar ist: Die europäischen Gesetzgeber haben die komplette Rechtsprechung überdacht, und es zeichnet sich ab, dass die Medizinprodukterichtlinien durch eine Medizinproduktverordnung abgelöst werden. Auf die daraus entstehenden Folgen für die Hersteller gehen wir in dieser zweiten Auflage ein. Des Weiteren wurden die benannten Stellen noch stärker zu unangekündigten Audits verpflichtet. Umso wichtiger ist es, dass die Hersteller die regulatorischen Forderungen einhalten, wozu dieses aktualisierte Buch ebenfalls beitragen wird.

Kontroverse Diskussionen innerhalb der EU haben dazu geführt, dass scheinbar über Nacht und ohne Übergangsfrist die Risikomanagementnorm EN 14971 zum 1. September 2012 überarbeitet wurde. Natürlich berücksichtigt das überarbeitete Kapitel 4 (»Risikomanagement«) diese Neuerung.

Doch nicht nur die Folgen regulatorischer Änderungen werden wir in dieser zweiten Auflage diskutieren, sondern auch auf aktuelle Trends wie die Mobile Medical Apps eingehen. Fehler in der ersten Auflage haben wir verbessert.

Christian Johner, Matthias Hölzer-Klüpfel, Sven Wittorf
Konstanz, Würzburg, Seeheim-Jugenheim, im Februar 2015

Vorwort zur 1. Auflage

Wenn sich 70 Personen aus ganz Deutschland zusammenfinden, um – ohne dass sie dafür in irgendeiner Weise vergütet würden – ein Thema zu besprechen, dann scheinen sie ein aufrichtiges und gemeinsames Anliegen zu haben.

Diese Personen, die bei Medizinprodukteherstellern, bei sogenannten benannten Stellen, in Krankenhäusern oder bei Trainingsanbietern arbeiten, stellen sich alle die gleichen Fragen:

Was müssen Entwickler, Auditoren, Betreiber oder Anwender von Medizinprodukten, die Software enthalten oder eigenständige medizinische Software sind, wissen und können? Welche Begriffe müssen sie kennen? Was müssen sie tun, um die rechtlichen Rahmenbedingungen einzuhalten und gleichzeitig effektiv und effizient zu arbeiten? Welche Dokumente müssen sie erstellen? Wie sollen sie das Risikomanagement anwenden? Wie kommen sie zu gebrauchstauglichen Produkten? Und am wichtigsten: Wie schaffen sie es, Software zu entwickeln, mit der die Anwender Patienten schnell und zuverlässig diagnostizieren, therapieren und überwachen können, ohne dabei die Anwender, Patienten und Dritte unnötig zu gefährden?

Es sind genau diese Fragen, die die 70 Personen verbinden, die zu den ersten Mitgliedern und Interessenten des Vereins »International Certified Professional for Medical Software Board« (ICPMSB) zählen. Daher haben sie sich in ihrem Verein das Ziel gesetzt, einen Kanon an Wissen und Fähigkeiten zu definieren und dafür Konzepte zur strukturierten Weiterbildung sowie zur Zertifizierung zu entwickeln.

Dass es dieser Weiterbildung dringend bedarf, wird gleich mehrfach schmerzlich deutlich: Zum einen steigt die Anzahl der Probleme mit Medizinprodukten ständig. So veröffentlicht das Bundesamt für Arzneimittel etwa zwei Hinweise der Hersteller zu Risiken mit Softwarebezug – pro Woche! Des Weiteren fehlt in den meisten Curricula der einschlägigen Hochschulstudiengänge wie Medizintechnik oder Medizininformatik das Thema »gesetzeskonforme Entwicklung medizinischer Software«. In Folge finden sich zahlreiche Firmen, die medizinische Software auf sehr »hemdsärmelige« Art entwickeln. Viele dieser Firmen drängen erstmalig in den für sie neuen Markt Gesundheitswesen. Das Gesund-

heitswesen ist inzwischen die größte Branche in Deutschland. Eine Branche, die sich dadurch auszeichnet, dass fehlerhafte Produkte besonders direkte und fatale Auswirkungen auf die Gesundheit und das Leben von Menschen haben können.

Möge dieses Buch dazu beitragen, dass die Medizinproduktehersteller ebenso wie deren Kunden (z.B. Krankenhäuser) medizinische Software künftig noch kompetenter, verantwortungsvoller und der Gesundheit von Patienten dienlicher entwickeln, betreiben und anwenden und so der gemeinsamen Verantwortung gerecht werden. Denn damit ginge ein großer Wunsch nicht nur der 70 Personen in Erfüllung.

All diesen unermüdlichen Helfern danken die Autoren von Herzen. Ohne sie wäre das Buch nicht entstanden. Sie werden auch für den weiteren Erfolg des Vereins wesentlich sein. Besonderer Dank gilt unseren Koautoren Thomas Geis, Dr. Christof Gessner und Markus Manleitner.

Allen Lesern, seien es Hersteller von Medizinprodukten, seien es Mitarbeiter von Krankenhäusern, Arztpraxen oder benannten Stellen, seien es Studenten oder Anbieter und Teilnehmer von Trainingsprogrammen, wünschen wir vor allem dies: viel Freude beim Lesen sowie viele Erkenntnisse und Anregungen, die sie direkt im beruflichen Alltag umsetzen können.

Christian Johner, Matthias Hölzer-Klüpfel, Sven Wittorf
Konstanz, Würzburg, Darmstadt, im Februar 2011

Inhaltsübersicht

1	Einleitung	1
2	Rechtliche Grundlagen	9
3	Qualitätsmanagement	71
4	Risikomanagement	83
5	Lebenszyklus medizinischer Software	119
6	Gebrauchstauglichkeit	171
7	Dokumentenmanagement	205
8	Medizinische Informatik	215
9	IT-Sicherheit bei Medizinprodukten	231

Anhang

Abkürzungsverzeichnis	249
Quellenverzeichnis	253
Index	257

Inhaltsverzeichnis

1	Einleitung	1
1.1	Aufbau dieses Buches	2
1.2	Initiative »Certified Professional for Medical Software« (CPMS)	3
1.3	Zuordnung der Kapitel dieses Buches zum Curriculum des CPMS	4
2	Rechtliche Grundlagen	9
2.1	Die Rechtslage in Europa	9
2.1.1	Das sogenannte neue Konzept für Produktregulierung innerhalb der Europäischen Union	9
2.1.2	Regulatorische Landkarte für Medizinprodukte	12
2.2	Regulatorische Vorgaben für Medizinprodukte	14
2.2.1	Die Medizinprodukterichtlinie und die Medizin- produkteverordnung	14
2.2.2	Besonderheiten für aktive implantierbare medizinische Geräte	33
2.2.3	Besonderheiten für In-vitro-Diagnostika	33
2.2.4	Die Gesetzgebung in der Bundesrepublik Deutschland	35
2.3	Harmonisierte Normen	39
2.3.1	Das neue Konzept der Europäischen Union	39
2.3.2	Entstehung von harmonisierten Normen	39
2.3.3	Veröffentlichung von harmonisierten Normen	40
2.4	Relevante harmonisierte Normen	40
2.4.1	Qualitätsmanagement (EN ISO 13485)	41
2.4.2	Risikomanagement (EN ISO 14971)	41
2.4.3	Software-Lebenszyklus-Prozesse (EN 62304)	41
2.4.4	Gebrauchstauglichkeit (EN 62366 und EN 60601-1-6)	42
2.4.5	Normenfamilie EN 60601 über medizinische elektrische Geräte	42

2.5	Anwendung und Kontrolle rechtlicher Vorgaben	45
2.5.1	Lebenszyklus eines Medizinproduktes	45
2.5.2	Überwachung von Herstellern	50
2.5.3	Überwachung von benannten Stellen	54
2.6	Weltweite Harmonisierungsbemühungen – die GHTF und das IMDRF	56
2.7	Die Situation in den USA	56
2.7.1	Aufbau der Gesetzgebung	57
2.7.2	Federal Food, Drug, and Cosmetic Act (FD&C Act)	58
2.7.3	Code of Federal Regulations Title 21 (21 CFR)	59
2.7.4	Food and Drug Administration (FDA)	60
2.7.5	Klassifizierung von Medizinprodukten	60
2.7.6	Inverkehrbringen von Medizinprodukten	61
2.7.7	Softwarespezifische Vorgaben	63
2.7.8	Vergleich mit Europa	67
2.8	Weitere internationale Behörden	68
3	Qualitätsmanagement	71
3.1	Aufbau der Norm ISO 13485	71
3.2	Prozessorientierter Ansatz	72
3.3	Dokumentationsanforderungen	72
3.3.1	Qualitätsmanagement-Handbuch	73
3.3.2	Zu dokumentierende Verfahren	73
3.3.3	Dokumente und Aufzeichnungen	74
3.4	Verantwortung der Leitung	75
3.5	Management von Ressourcen	75
3.6	Produktrealisierung	76
3.6.1	Planung	76
3.6.2	Einbindung des Kunden	76
3.6.3	Design und Entwicklung	77
3.6.4	Beschaffung	78
3.6.5	Produktion und Dienstleistungserbringung	78
3.6.6	Umgang mit Kundeneigentum	79
3.6.7	Überwachung von Messmitteln	80
3.7	Messung, Analyse und Verbesserung	80
3.7.1	Sammeln von Rückmeldungen	80
3.7.2	Internes Audit	81
3.7.3	Messung von Prozessen	81

3.7.4	Fehlerhafte Produkte	81
3.7.5	Verbesserung	81
4	Risikomanagement	83
4.1	Einführung	83
4.1.1	Regulatorischer Rahmen	83
4.1.2	Bedeutung des Risikomanagements	85
4.1.3	Begriffe	85
4.2	Die Risikobewertungsmatrix	89
4.2.1	Definition der Achsen	90
4.2.2	Risikoakzeptanz	92
4.3	Verfahren zur Risikoanalyse	92
4.3.1	Vorläufige Gefährdungsanalyse (PHA)	92
4.3.2	Fehlerbaumanalyse (FTA)	95
4.3.3	Fehlermöglichkeits- und -einflussanalyse (FMEA)	96
4.3.4	Abschätzen von Wahrscheinlichkeit und Schweregrad ...	98
4.4	Die ISO 14971	99
4.4.1	Allgemeine Anforderungen an das Risikomanagement ...	99
4.4.2	Der Risikomanagementprozess	101
4.4.3	Dokumentation	107
4.5	Zusammenspiel mit anderen Normen	109
4.5.1	Zusammenspiel mit der ISO 13485	109
4.5.2	Zusammenspiel mit der IEC 62304	110
4.5.3	Zusammenspiel mit der IEC 62366-1	111
4.6	Risikomanagement bei Software	112
4.6.1	Definition Softwaresicherheitsklassen	112
4.6.2	Wahrscheinlichkeit und Softwaresicherheitsklassen	114
4.6.3	Dekomposition des Softwaresystems	115
4.6.4	Einflüsse auf die Architektur	116
4.7	Zusammenfassung	117
5	Lebenszyklus medizinischer Software	119
5.1	Softwareentwicklungsprozesse	119
5.1.1	Regulatorische Anforderungen	119
5.1.2	Vorgehensmodelle	119
5.1.2.1	Einführung	119
5.1.2.2	Wasserfallmodell	121
5.1.2.3	V-Modell	122
5.1.2.4	Iterativ-inkrementelle Modelle	123

5.1.3	Prozessbeschreibung	124
5.1.3.1	Einführung	124
5.1.3.2	Prozessgebiete festlegen	125
5.1.4	Konformitätsnachweis	126
5.1.4.1	Einführung	126
5.1.4.2	Audits bestehen	126
5.2	Softwareentwicklung	127
5.2.1	Entwicklungsplanung	127
5.2.1.1	Einführung	127
5.2.1.2	Softwareentwicklung planen	127
5.2.1.3	Entwicklungsprozesse anpassen	128
5.2.1.4	Standards, Methoden und Werkzeuge auswählen	128
5.2.1.5	Projekte planen	129
5.2.2	Softwareanforderungsanalyse	129
5.2.2.1	Einführung	129
5.2.2.2	Softwareanforderungen ableiten	130
5.2.2.3	Softwareanforderungen formulieren	131
5.2.2.4	Softwareanforderungen verifizieren	133
5.2.3	Softwarearchitektur	134
5.2.3.1	Einführung	134
5.2.3.2	Softwarearchitektur beschreiben	135
5.2.3.3	Sicherheitsklasse reduzieren	138
5.2.3.4	Risikobehandlung sicherstellen	139
5.2.3.5	SOUP einsetzen	140
5.2.3.6	Softwarearchitektur verifizieren	140
5.2.4	Softwaredesign	141
5.2.4.1	Einführung	141
5.2.4.2	Softwaredesign beschreiben	142
5.2.4.3	Schnittstellen definieren	143
5.2.4.4	Design verifizieren	143
5.2.5	Implementierung	143
5.2.5.1	Einführung	143
5.2.5.2	Softwareeinheiten implementieren	144
5.2.5.3	Akzeptanzkriterien festlegen	144
5.2.5.4	Codierrichtlinien einsetzen	145
5.2.5.5	Softwareeinheiten verifizieren	145
5.2.6	Integration	146
5.2.6.1	Einführung	146
5.2.6.2	Software-Build beherrschen	147
5.2.6.3	Integrationsstrategie festlegen	148
5.2.6.4	Integration verifizieren	148

5.2.7	Softwaretest	149
5.2.7.1	Einführung	149
5.2.7.2	Testebenen auswählen	149
5.2.8	Tests planen	150
5.2.8.1	Tests durchführen	150
5.2.8.2	Tests verifizieren	151
5.2.8.3	Änderungen prüfen	152
5.2.9	Freigabe	152
5.2.9.1	Einführung	152
5.2.9.2	Entwicklung abschließen	153
5.2.9.3	Software archivieren	153
5.2.9.4	Validierung durchführen	154
5.3	Softwarekonfigurationsmanagement	156
5.3.1	Einführung	156
5.3.2	Konfigurationskontrolle	156
5.3.2.1	Konfigurationselemente identifizieren	156
5.3.2.2	Elemente und Versionen kennzeichnen	157
5.3.2.3	Versionskontrollsystem nutzen	157
5.3.2.4	Softwareversionen benennen	159
5.3.2.5	SOUP identifizieren	160
5.3.3	Änderungskontrolle	161
5.3.3.1	Änderungsanforderungen genehmigen	161
5.3.3.2	Änderungen implementieren	161
5.3.3.3	Rückverfolgbarkeit sicherstellen	162
5.4	Softwareproblemlösung und -wartung	162
5.4.1	Einführung	162
5.4.2	Softwareproblemlösung	163
5.4.2.1	Problembereiche erstellen	163
5.4.2.2	Probleme lösen	164
5.4.2.3	Problemlösung verifizieren	165
5.4.2.4	Trends analysieren	165
5.4.3	Softwarewartung	165
5.4.3.1	Wartung planen	165
5.4.3.2	Rückmeldungen behandeln	166
5.4.3.3	Änderung implementieren	167
5.4.3.4	Software freigeben	168
5.5	Umgang mit älterer Software	168
5.5.1	Einführung	168
5.5.2	Risikomanagement	169
5.5.2.1	Rückmeldungen auswerten	169
5.5.2.2	Risikomanagementaktivitäten durchführen	169

5.5.3	Umgang mit Lücken	169
5.5.3.1	Lücken identifizieren	169
5.5.3.2	Aktivitäten planen	170
5.5.3.3	Lücken schließen	170
5.5.4	Dokumentation	170
5.5.4.1	Version dokumentieren	170
5.5.4.2	Nutzung begründen	170
6	Gebrauchstauglichkeit	171
6.1	Einführung	171
6.1.1	Bedeutung der gebrauchstauglichkeitsorientierten Entwicklung	171
6.1.2	Übersicht	172
6.1.3	Definitionen	173
6.2	Regulatorisches Umfeld	175
6.2.1	EU-Verordnungen, Gesetze und Behörden	175
6.2.2	Normen	177
6.3	Weg zu validen Anforderungen	180
6.3.1	Benutzer identifizieren und charakterisieren	181
6.3.2	Kontext erheben und Zweckbestimmung festlegen	182
6.3.3	Nutzungsanforderungen ableiten	182
6.4	Benutzungsschnittstelle konzipieren	185
6.4.1	Nutzungsszenarien für jede zu unterstützende Kernaufgabe konstruieren	185
6.4.2	Benutzungsschnittstelle spezifizieren	186
6.4.3	Prototyp entwerfen und prüfen	189
6.5	Prüfung: Verifizierung und Validierung	190
6.5.1	Inspektionsverfahren	190
6.5.2	Teilnehmende Beobachtung (Usability-Test)	194
6.5.3	Qualitative und quantitative Benutzerbefragungen	195
6.5.4	Zusammenfassung der Prüfverfahren	195
6.6	IEC-62366-1-konforme Dokumentation	196
6.6.1	Gebrauchstauglichkeitsorientierter Entwicklungsprozess	196
6.6.2	Gebrauchstauglichkeitsakte	198
6.7	UOUP: Benutzer-Produkt-Schnittstellen unbekannter Herkunft . . .	202
6.8	Zusammenfassung	203

7	Dokumentenmanagement	205
7.1	Einführung	205
7.2	Allgemeine Anforderungen an Dokumente	205
7.3	Geforderte Dokumentation	207
7.3.1	Qualitätsmanagement	207
7.3.2	Risikomanagementakte	208
7.3.3	Gebrauchstauglichkeitsakte	208
7.3.4	Dokumentation der Softwareentwicklung	209
7.3.5	Technische Dokumentation	210
7.3.6	Sonstige Dokumente	211
7.3.7	Übersicht über geforderte Dokumente	211
7.4	Umgang mit Dokumenten	212
7.5	Zusammenfassung	214
8	Medizinische Informatik	215
8.1	Einführung	215
8.1.1	Gesundheitswesen	215
8.1.2	Informationssysteme	217
8.2	Interoperabilität	218
8.2.1	Interoperabilitätsebenen	218
8.2.2	Kommunikationsstandards	220
8.2.3	Semantische Standards	229
8.3	Zusammenfassung	230
9	IT-Sicherheit bei Medizinprodukten	231
9.1	Einführung	231
9.1.1	Probleme mit der IT-Sicherheit	231
9.1.2	IT-Sicherheit: Begriffsdefinition und Ziele	231
9.1.3	Das STRIDE-Modell	233
9.2	Regulatorische Rahmen	233
9.2.1	MDR und IVDR	233
9.2.2	Normen	234
9.2.3	MDCG 2019-16	235
9.2.4	Nationale Vorgaben für Medizinprodukte	235
9.2.5	Vorgaben an die IT-Sicherheit, die nicht spezifisch für Medizinprodukte gelten	236

9.3	IT-Sicherheit im Produktlebenszyklus	236
9.3.1	Allgemeines	236
9.3.2	Zweckbestimmung und Stakeholder-Anforderungen	237
9.3.3	System- und Softwareanforderungen	237
9.3.4	System- und Softwarearchitektur	240
9.3.5	Testaktivitäten	241
9.3.6	Softwarefreigabe	241
9.3.7	Überwachung des Produktes im Markt nach dem Inverkehrbringen	242
9.4	Produktanforderungen	243
9.4.1	Authentifizierung und Autorisierung	243
9.4.2	Daten und Kommunikation	244
9.4.3	Audit-Log	244
9.4.4	Begleitmaterialien	245
9.5	Zusammenfassung	245

Anhang

Abkürzungsverzeichnis	249
Quellenverzeichnis	253
Index	257

1 Einleitung

In atemberaubender Geschwindigkeit wächst der Anteil der Wertschöpfung, der durch Software generiert wird. Das gilt auch für den Markt der Medizinprodukte. Besonders offenbart sich dieser Trend bei eigenständiger Software wie Diagnose- oder Therapieplanungssystemen. Aber auch bei vielen klassischen Medizingeräten hängt die Wettbewerbsfähigkeit davon ab, wie schnell und zuverlässig Informationen verarbeitet und dem medizinischen Personal zur Verfügung gestellt werden. Das betrifft beispielsweise die Bildverarbeitung in CTs oder Kernspingeräten ebenso wie die Navigationssysteme für die Chirurgie.

Als weiterer Trend lässt sich das Zusammenwachsen von Medizintechnik und Medizin-IT beobachten: Es gibt kaum ein Medizingerät, das nicht in ein Netzwerk einzubinden ist und das nicht mit klinischen Informationssystemen Daten austauschen muss. Die viel diskutierte Telematikinfrastruktur zielt sogar auf eine deutschlandweite Vernetzung von medizinischen Systemen.

Dieser technologische Fortschritt bedeutet jedoch nicht nur große Chancen im Sinne einer wirkungsvolleren, schnelleren und kosteneffizienteren Diagnostik und Therapie. Er bedeutet auch zusätzliche Risiken für Patienten, Anwender und Dritte. Diese Risiken führen zu Gesundheitsschädigungen – bis hin zum Tod. Künftige Entwicklungen wie die personalisierte Medizin, die auf Methoden der Bioinformatik und Molekularmedizin basiert, werden es sicher nicht einfacher machen, ein ausgewogenes Chancen-Risiko-Verhältnis dieser neuen Technologien und Verfahren zu wahren.

Als Reaktion auf vermehrte Probleme, vor allem mit Bezug zur Software, verschärfen viele Länder seit nun fast einem Jahrzehnt die regulatorischen Vorgaben.

- Im Jahr 2010 wurde das Medizinproduktegesetz (MPG) novelliert.
- Im Jahr 2010 wurde die Norm IEC 80001-1 über das Risikomanagement von IT-Netzwerken verabschiedet.
- 2012 erschien die ISO 14971:2012, in der Risiken nicht mehr einfach als akzeptabel klassifiziert werden dürfen.
- Seit 2013 haben die benannten Stellen (verstärkt) begonnen, unangekündigte Audits durchzuführen.

- Die FDA hat in diesen Jahren zahlreiche Guidance-Dokumente veröffentlicht u. a. zu Medical Apps, zur Cybersecurity und zum Thema künstliche Intelligenz.
- Die Auditoren bauen die eigene Softwarekompetenz aus und verschärfen die Audits.
- Seit dem Jahr 2017 werden die Medizinprodukterichtlinien nach und nach durch Verordnungen abgelöst. Diese legen wesentlich strengere Maßstäbe an den Nachweis der Wirksamkeit von Medizinprodukten an und erhöhen massiv die Verpflichtungen für alle Wirtschaftsakteure im Gesundheitswesen, die mit Medizinprodukten umgehen.

Diese erhöhten regulatorischen Anforderungen führen aber nicht zwangsläufig und unmittelbar zu besseren, weil sicheren Medizinprodukten. Sie führen jedoch in den meisten Fällen zu einem erhöhten Aufwand bei Herstellern und Betreibern, besonders die Dokumentation betreffend. Häufig empfinden es beide als einen Spagat, die regulatorischen Anforderungen erfüllen zu müssen und den dabei entstehenden Aufwand vertretbar zu halten.

1.1 Aufbau dieses Buches

In den folgenden Kapiteln will dieses Buch darlegen, dass es hier nicht notwendigerweise um einen Kompromiss geht, sondern es will Wege aufzeigen, mit denen eine Entwicklung (und der Betrieb) nach Best Practices implizit zur Gesetzeskonformität und gleichzeitig zu einem effektiven, kosten- und zeitsparenden Arbeiten führt. Und genau das möchten die Autoren der Normen auch erreichen. Es geht somit nicht um Kompromisse, sondern vielmehr um eine Portion gesunden Menschenverstand.

Kapitel 2 führt in die rechtlichen Grundlagen ein. Diese zu kennen und zu verstehen ist die Grundvoraussetzung für das Verständnis der weiteren Kapitel. Nach dem Lesen dieses Kapitels sollte es klarer sein, wie Richtlinien, Gesetze, Verordnungen und Normen ineinandergreifen und wo man bei welchen Fragen nachschauen muss.

Kapitel 3 stellt die ISO 13485 vor. Diese Norm nennt Anforderungen an ein Qualitätsmanagement und ist für die medizinische Software die unspezifischste Norm. Sie gibt jedoch den »großen Rahmen« vor.

Alle für medizinische Software relevanten Normen verweisen auf das Risikomanagement. Ohne ein adäquates Risikomanagement lässt sich kein Audit bestehen. Nur wer die Risiken seines Medizinproduktes kennt, kann viele Fragen beantworten, die im Laufe der Spezifikation, beim Entwickeln und dem Testen von medizinischer Software auftauchen. Daher widmet sich das Kapitel 4 ausschließlich dem Thema Risikomanagement und stellt die entsprechenden Bezüge zu den folgenden Kapiteln her.

Zu diesen Kapiteln zählt das Kapitel 5 zum Lebenszyklus medizinischer Software. Hier geht es sowohl um Aspekte und Best Practices des Software Engineering als auch um die Forderungen der IEC 62304. Für Softwarearchitekten und Programmierer wird dieses Kapitel eines der wichtigsten sein.

Das wahrscheinlich am meisten unterschätzte und gleichzeitig das bedeutendste Thema ist die »Usability«, die Gebrauchstauglichkeit, der Medizinprodukte. Fast alle Hersteller glauben zu wissen, was ihre Kunden benötigen, glauben, dass man durch ein Befragen dieser zu den Anforderungen kommt. Die Alltagsrealität kennt aber Feststellungen wie »die Kunden wollen jetzt etwas anderes« oder »es gibt neue oder geänderte Anforderungen«. Und genau diese Feststellungen sind ein trauriger Beweis des Gegenteils. Ebenso wie die Statistik der FDA, die 70 % aller softwarebezogenen Rückrufe auf mangelnde Gebrauchstauglichkeit zurückführt. Aus diesem Grund geht das Kapitel 6 dediziert auf dieses Thema und die dazu relevanten Normen ein, die IEC 60601-1-6 und IEC 62366.

Gleichsam als verbindende Klammer um die vorangegangenen Kapitel dient das Kapitel 7 zum Dokumentenmanagement. Es hat zum Ziel, die wichtigsten Anforderungen an die Erstellung und Lenkung von Dokumenten zu erläutern und Hinweise zu einer Dokumentenlandschaft, also dem Aufteilen der Dokumente auf die verschiedenen Akten, zu geben.

Medizinprodukte sind wie oben beschrieben heute nur selten als isolierte Systeme zu sehen. Vielmehr müssen sie in einen Verbund aus anderen Medizingeräten und Informationssystemen integriert werden und mit diesen zusammenspielen. Die Interoperabilität ist somit eine wesentliche Voraussetzung. Kapitel 8 »Medizinische Informatik« geht der Frage nach, welche Systeme wie zu integrieren sind und welche Standards und Klassifikationen es auf den unterschiedlichen Integrationsebenen zu kennen und zu beachten gilt. Das 2020 in den Lehrplan aufgenommene Thema »IT-Sicherheit« wird in Kapitel 9 behandelt.

1.2 Initiative »Certified Professional for Medical Software« (CPMS)

Genauso wie Normen helfen sollen, einheitliche Standards – in diesem Fall bei der Entwicklung medizinischer Software – zu schaffen, können Zertifizierungsprogramme dazu beitragen, einen einheitlichen Kanon an Wissen zu definieren, über den Personen verfügen sollen, die medizinische Software normen- und gesetzeskonform entwickeln, zulassen oder betreiben. Solch ein Kanon wird nur dann Anerkennung finden, wenn er durch ein unabhängiges Gremium erarbeitet, weiterentwickelt und geprüft wird.

Genau dieses Ziel hat sich der Verein »International Certified Professional for Medical Software Board e.V.« (ICPMSB e.V.) gesetzt. Seine Mitglieder – z.B. Vertreter von Herstellern, benannten Stellen, Trainingsanbietern und Beratern – definieren die Lehrinhalte, Lernziele und Prüfungsmodalitäten. Der Verein akkre-

ditiert Trainingsanbieter und Institutionen, welche die Prüfungen abnehmen, und stellt so eine Einheitlichkeit und Vergleichbarkeit der Lehr- und Prüfungsinhalte sowie Prüfungsmodalitäten sicher.

Dieses Buch basiert auf dem Curriculum, welches das Gremium des ICPMSB e.V.¹ erarbeitet hat, das die Lehrinhalte und Lernziele definiert. Seine Kapitelstruktur deckt sich mit den Modulen des Basiscurriculums.

1.3 Zuordnung der Kapitel dieses Buches zum Curriculum des CPMS

Die folgende Tabelle listet die bei Drucklegung gültige Kapitelstruktur des CPMS (v3.0) auf und verweist auf das Kapitel innerhalb dieses Buches, in dem die dortigen Themen behandelt werden. Da sich die Lernziele und die Struktur des Lehrplans mit fortschreitenden Veränderungen der Regularien ebenfalls verändern werden, ist eine jeweils aktuelle Tabelle online unter *www.dpunkt.de/cpms* verfügbar.

CPMS Curriculum v3.0		Buchkapitel
Kapitel	Titel	
1	Curriculum Regulatorische Landschaft	Kapitel 2
1.1	Rechtliche Grundlagen	Abschnitt 2.1 und 2.3
1.1.1	Begriffe und Akteure	Abschnitt 2.1.1
1.1.2	Rechtliche Grundlagen in Europa	Abschnitt 2.1.1 und 2.3
1.2	Die europäischen Verordnungen	Abschnitt 2.2.1
1.2.1	Die Medizinprodukteverordnung (MDR)	Abschnitt 2.2.1
1.2.3	Umsetzung in nationales Recht	Abschnitt 2.2.4
1.3	Die harmonisierten Normen	Abschnitt 2.3 und 2.4
1.3.1	EN ISO 13485	Abschnitt 2.4.1
1.3.2	EN ISO 14971	Abschnitt 2.4.2
1.3.3	EN 62304	Abschnitt 2.4.3
1.3.4	EN 62366	Abschnitt 2.4.4
1.3.5	Die Normenfamilie EN 60601-x	Abschnitt 2.4.5
1.4	Kontrollen	Abschnitt 2.5
1.4.1	Kontrollen im Lebenszyklus eines Medizinprodukts	Abschnitt 2.5
1.4.2	Überwachung durch Behörden und Benannte Stellen	Abschnitt 2.5
1.5	Regularien außerhalb der EU	Abschnitt 2.7 und 2.8
1.5.1	Regulatorische Grundlagen für den US-Markt	Abschnitt 2.7
1.5.2	Zulassungsverfahren in anderen Ländern	Abschnitt 2.8

→

1. <http://www.icpmsb.org/>

CPMS Curriculum v3.0		Buchkapitel
Kapitel	Titel	
2	Curriculum Risikomanagement	Kapitel 4
2.1	Einführung in das Risikomanagement	Abschnitt 4.1
2.1.1	Regulatorische Forderungen	Abschnitt 4.1.1
2.1.2	Begriffsdefinitionen	Abschnitt 4.1.2
2.1.3	Risikomanagementplanung	Abschnitt 4.1.2
2.1.4	Risikomanagementakte	Abschnitt 4.4.3
2.2	Der Risikomanagement-Prozess nach ISO 14971	Abschnitt 4.4
2.2.1	Allgemeine Anforderungen	Abschnitt 4.4.2
2.2.2	Der Risikomanagementprozess	Abschnitt 4.4.2
2.2.3	Zweckbestimmung und bestimmungsgemäßer Gebrauch	Abschnitt 4.4.2
2.2.4	Gefährdungs- und Risikoanalyse	Abschnitt 4.4.2
2.2.5	Risikobewertungsmatrix	Abschnitt 4.2
2.2.6	Risikobewertung und Risikoakzeptanz	Abschnitt 4.2.2 und 4.4.2
2.2.7	Risikobeherrschung	Abschnitt 4.4.3
2.2.8	Risiko-/Nutzenbewertung	Abschnitt 4.4.2
2.2.9	Gesamt-Restrisiko und Risikomanagementbericht	Abschnitt 4.4.3
2.2.10	Nachgelagerte Phase	Abschnitt 4.4.2
2.3	Verfahren zur Risikoanalyse	Abschnitt 4.3
2.3.1	Grundlegendes zu Risikoanalyse	Abschnitt 4.3
2.3.2	Preliminary Hazard Analysis	Abschnitt 4.3.1
2.3.3	Fault Tree Analysis	Abschnitt 4.3.2
2.3.4	Failure Mode and Effects Analysis (FMEA)	Abschnitt 4.3.3
2.4	Dokumentation	Abschnitt 4.4.3
2.5	Risikomanagement bei Software	Abschnitt 4.3 und 4.4
2.6	IEC 80002-1	Abschnitt 4.5.2
3	Curriculum Software-Engineering	Kapitel 5
3.1	Softwareentwicklungsprozesse	Abschnitt 5.1
3.2	Entwicklungsplanung	Abschnitt 5.2.1
3.3	Software-Anforderungsanalyse	Abschnitt 5.2.2
3.3.1	Anforderungen ermitteln	Abschnitt 5.2.2.2
3.3.2	Anforderungen dokumentieren	Abschnitt 5.2.2.3
3.3.3	Anforderungen verifizieren	Abschnitt 5.2.2.4
3.3.4	Anforderungen verwalten	Abschnitt 5.2.2

CPMS Curriculum v3.0		Buchkapitel
Kapitel	Titel	
3.4	Softwarearchitektur	Abschnitt 5.2.3
3.4.1	Softwarearchitektur beschreiben	Abschnitt 5.2.3.2
3.4.2	Sicherheitsklassen	Abschnitt 5.2.3.3 und 4.6
3.4.3	Risikobehandlung sicherstellen	Abschnitt 5.2.3.4
3.4.4	Softwarearchitektur verifizieren	Abschnitt 5.2.3.6
3.5	SW-Design	Abschnitt 5.2.4
3.5.1	Softwaredesign beschreiben	Abschnitt 5.2.4.1
3.5.2	Schnittstellen definieren	Abschnitt 5.2.4.3
3.5.3	Design verifizieren	Abschnitt 5.2.4.4
3.6	SW-Implementierung	Abschnitt 5.2.5
3.6.1	Softwareeinheiten implementieren	Abschnitt 5.2.5.2
3.6.2	Akzeptanzkriterien festlegen	Abschnitt 5.2.5.3
3.6.3	Codierrichtlinien einsetzen	Abschnitt 5.2.5.4
3.6.4	Softwareeinheiten verifizieren	Abschnitt 5.2.5.5
3.7	Software-Integration	Abschnitt 5.2.6
3.8	Softwaretest	Abschnitt 5.2.7 und 5.2.8
3.8.1	Allgemeine Anforderungen aus der IEC 62304	Abschnitt 5.2.7 und 5.2.8
3.8.2	Verifizierung vs. Validierung	Abschnitt 5.2.9.4
3.9	Software-Freigabe	Abschnitt 5.2.9
3.10	Softwarekonfigurationsmanagement (im LP alt 5.2)	Abschnitt 5.3
3.10.1	Konfigurationselemente	Abschnitt 5.3.1
3.10.2	Notwendigkeit des Konfigurationsmanagements	Abschnitt 5.3.1
3.10.3	Konfigurationselemente identifizieren	Abschnitt 5.3.2.2
3.10.4	Werkzeuge für das Konfigurationsmanagement	Abschnitt 5.3.2.3
3.10.5	Konfigurationsmanagementplan	Abschnitt 5.3.2.1
3.10.6	Änderungsmanagement	Abschnitt 5.3.3
3.11	Software-Wartung	Abschnitt 5.4
3.11.1	Planung der Software-Wartung	Abschnitt 5.4.3.2
3.11.2	Analyse von Problemen und Änderungen	Abschnitt 5.4.3.2 und 5.4.3.3
3.11.3	Implementierung von Änderungen	Abschnitt 5.4.3.3 und 5.4.3.4
3.12	Software-Problemlösung	Abschnitt 5.4
3.13	Traceability im SW-Entwicklungsprozess	Abschnitt 5.2.2.4
3.13.1	Grundlagen	Abschnitt 5.2.2.4
3.13.2	Tracing durchführen	Abschnitt 5.2.2.4

CPMS Curriculum v3.0		Buchkapitel
Kapitel	Titel	
3.14	Software of Unknown Provenance (SOUP)	Abschnitt 5.2.3.5
3.14.1	Definition und Beispiele für SOUP	Abschnitt 5.2.3.5
3.14.2	Umgang mit Software of Unknown Provenance	Abschnitt 5.3.2.5, 4.3.3, 5.4.3.1 und 5.2.3.5
4	Curriculum Usability	Kapitel 6
4.1	Grundlagen Usability	Abschnitt 6.1
4.1.1	Allgemeine Anforderungen	Abschnitt 6.1.1
4.1.2	Begrifflichkeiten im Kontext der Gebrauchstauglichkeit	Abschnitt 6.1.3 und 6.2.2
4.2	Regulatorische Forderungen	Abschnitt 6.2
4.2.1	Regulatorische Anforderungen (Europa)	Abschnitt 6.2.1
4.2.2	Normen und weitere Richtlinien	Abschnitt 6.2.2
4.3	Forderungen der IEC 62366-1	Abschnitt 6.2.2
4.4	Vom Nutzungskontext zu Nutzungsanforderungen	Abschnitt 6.3
4.4.1	Grundlagen	Abschnitt 6.3.1
4.4.2	Nutzungskontext	Abschnitt 6.3.2
4.4.3	Ableiten der Nutzungsanforderungen	Abschnitt 6.3.3
4.5	Benutzungsschnittstelle	Abschnitt 6.4
4.5.1	Benutzungsschnittstelle konzipieren	Abschnitt 6.4.2
4.5.2	Benutzungsschnittstelle und Risiken	Abschnitt 6.6.2
4.6	Methoden der Evaluierung	Abschnitt 6.5
4.6.1	Grundlagen	Abschnitt 6.5
4.6.2	Formative Evaluation	Abschnitt 6.5
4.6.3	Summative Evaluation	Abschnitt 6.5
4.7	Dokumentation	Abschnitt 6.6
5	Curriculum Qualitäts- und Dokumentenmanagement	Kapitel 3 und 7
5.1	Qualitätsmanagement	Kapitel 3
5.1.1	Prozessorientierter Ansatz	Abschnitt 3.2
5.1.2	Dokumentationsanforderungen an das Qualitätsmanagementsystem	Abschnitt 3.3
5.2	Allgemeine Anforderungen an die Dokumentation	Kapitel 7
5.2.1	Lebenszyklus von Dokumenten und Aufzeichnungen	Abschnitt 7.4
5.2.2	Anforderungen an die Erstellung von Dokumenten	Abschnitt 7.2
5.2.3	Anforderungen an die Prüfung und Freigabe von Dokumenten	Abschnitt 7.4

CPMS Curriculum v3.0		Buchkapitel
Kapitel	Titel	
5.3	Geforderte Dokumentation	Abschnitt 7.3
5.3.1	Grundlagen	Abschnitt 7.3
5.3.2	Die Technische Dokumentation	Abschnitt 7.3.5
6	Curriculum Medizinische Informatik	Kapitel 8
6.1	Informatik im Gesundheitswesen	Abschnitt 8.1.1
6.1.1	Grundlagen	Abschnitt 8.1.1
6.1.2	Daten im Gesundheitswesen	Abschnitt 8.1.1
6.1.3	Informationssysteme	Abschnitt 8.1.2
6.2	Interoperabilität	Abschnitt 8.2
6.2.1	Prinzipien der Interoperabilität	Abschnitt 8.2.1
6.2.2	Ordnungssysteme	Abschnitt 8.2.3
6.2.3	Interoperabilität medizinischer Daten	Abschnitt 8.2.2
6.2.4	Interoperabilität von Nachrichten	Abschnitt 8.2.2
6.2.5	Interoperabilität von Prozessen	Abschnitt 8.2.2
6.2.6	Praktische Umsetzung der Interoperabilität	Abschnitt 8.2
7	Curriculum IT Security	Kapitel 9
7.1	Allgemeine Anforderungen	Abschnitt 9.1 und 9.2
7.2	Anforderungen an die Prozesse	Abschnitt 9.3
7.3	Anforderungen an das Produkt	Abschnitt 9.4

2 Rechtliche Grundlagen

Dieses Kapitel beschreibt die rechtlichen Rahmenbedingungen, unter denen in Deutschland und international Medizinprodukte entwickelt werden müssen. Es wirft zunächst einen Blick auf die Rechtslage in Europa und erläutert danach die europäischen Regularien, die sich mit Medizinprodukten beschäftigen. Es fasst die anwendbaren Normen zur Erfüllung dieser Regularien zusammen. Die nachfolgenden Kapitel dieses Buches gehen im Detail darauf ein und zeigen auf, wie diese regulatorischen Vorgaben die Planung, Entwicklung und Herstellung eines Medizinproduktes beeinflussen. Nach der Schilderung der Situation in Europa gibt der letzte Teil dieses Kapitels einen Überblick über internationale Anstrengungen und die Situation in den USA.

Neueinsteiger in die Thematik sollten dieses Kapitel von Anfang bis Ende durchlesen und sich nicht von der hohen Informationsdichte abschrecken lassen. Erfahreneren Lesern soll es als Nachschlagemöglichkeit dienen.

2.1 Die Rechtslage in Europa

2.1.1 Das sogenannte neue Konzept für Produktregulierung innerhalb der Europäischen Union

Eines der großen europäischen Ziele ist der Abbau von Handelshemmnissen innerhalb des europäischen Binnenmarktes und die technische Harmonisierung bestimmter Produktgruppen. Hierzu wurde 1985 das sogenannte »neue Konzept« (engl. New Approach) eingeführt¹. Im Sinne dieses neuen Konzeptes wurden seitdem für über 30 Produktgruppen europäische Richtlinien und Verordnungen erstellt. Neben Medizinprodukten sind dies z.B. Spielzeuge, Messgeräte, einfache Druckbehälter, Maschinen, Verpackungen und Verpackungsabfälle, Explosivstoffe für zivile Zwecke, Sportboote oder Aufzüge. Diese Richtlinien und Verordnungen beruhen auf den folgenden Prinzipien²:

1. Siehe https://de.wikipedia.org/wiki/Neues_Konzept_f%C3%BCr_die_Produktkonformit%C3%A4t_in_der_Europ%C3%A4ischen_Union.
2. Zitiert aus dem »Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfaßten Richtlinien«, erstellt von der Europäischen Kommission.